

Automorphism Groups of Hyperbolic Lattices

Michael H. Mertens^{*}

Mathematisches Institut der Universität zu Köln,

Weyertal 86-90,

D-50931 Köln, Germany

Phone: +49 – (0)221/4704333

E-Mail: mmertens@math.uni-koeln.de

<http://www.mi.uni-koeln.de/~mmertens/>

April 17, 2013

Abstract

Based on the concept of dual cones introduced by J. Opgenorth we give an algorithm to compute a generating system of the group of automorphisms of an integral lattice endowed with a hyperbolic bilinear form.

1 Introduction

In his famous paper *Nouvelles applications des paramètres continus à la théorie des formes quadratiques* [20], G. F. Voronoi presented an algorithm to enumerate (up to scaling) all perfect quadratic forms in a given dimension n . The general idea for that was to compute a face-to-face tessellation of a certain cone in the space of symmetric endomorphisms of \mathbb{R}^n based on the pyramids induced by the shortest vectors of a perfect quadratic form.

Generalizing Voronoi's ideas, M. Koecher came up with the concept of *self-dual cones* or, as he called them, *positivity domains* [7, 8] to obtain an alternative to the reduction theory of quadratic forms due to H. Minkowski.

Another slight generalization of these ideas to so called *dual cones* was then suiting for J. Opgenorth to find an algorithm to determine a generating system for the normalizer $N_{\mathrm{GL}_n(\mathbb{Z})}(G)$ of a finite unimodular group G of degree n (cf. [13]), which is an essential tool e.g. dealing with crystallographic space groups (cf. [14]).

^{*}The results in this paper are partially contained in the author's master's thesis [10] written under the supervision of Prof. Dr. Gabriele Nebe at Lehrstuhl D für Mathematik, RWTH Aachen University, Templergraben 64, D-52062 Aachen, Germany

[†]The author's research is supported by the DFG Graduiertenkolleg 1269 "Global Structures in Geometry and Analysis"

The goal here is to use these methods to derive an algorithm which gives a generating system of the automorphism group of an integral hyperbolic lattice¹ (L, Φ) (see Notation below).

There exists an algorithm due to E.B. Vinberg [19] to construct the maximal normal subgroup of the automorphism group of a hyperbolic lattice that is generated by reflections. But this algorithm terminates if and only if this reflection group has finite index in the full automorphism group, i.e. the lattice L is called *reflective*. But reflective lattices are very rare: For example if we consider the lattice \mathbb{Z}^n together with the bilinear forms induced by matrices

$$H_n^{(d)} := \text{diag}(-d, 1, \dots, 1) \in \mathbb{Z}^{n \times n} \text{ for } d > 0,$$

then it is known, that $(\mathbb{Z}^n, H_n^{(1)})$ is reflective if and only if $n \leq 19$ (cf. [19]). According to the classification of reflective hyperbolic lattices of rank 3 by D. Allock in [1], the highest prime divisor of the discriminant of such a lattice is 97 (cf. [1, p. 24]). Thus reflective lattices can neither occur in high dimensions nor for high discriminants.

To the author's knowledge so far there is no algorithm known to determine the automorphism group of a general hyperbolic lattice. The algorithm presented in this paper does at least not have theoretical limitations although in practice it can only handle lattices of small ranks (up to 4 in general, some examples of rank up to 7 work as well) and moderate discriminants.

The paper will be organized as follows: In Section 2 we recall the basic definitions and key results about dual cones from [13] which give a general method to determine generating systems of discontinuous groups acting on dual cones. The application of the results in Section 2 on hyperbolic lattices as well as a quite powerful way to shorten the calculation time is given in Section 3. Some examples and statistics are presented in Section 4. These were calculated using the computer algebra system MAGMA (cf. [3]). The source code for the necessary MAGMA-package `Authyp.m` as well as a short description of the included intrinsics is available via the author's homepage <http://www.mi.uni-koeln.de/~mmertens>.

Notation A *lattice* (L, Φ) always consists of two data, a free \mathbb{Z} -module L of rank n with basis $B = (b_1, \dots, b_n)$ and a non-degenerate, symmetric bilinear form $\Phi : \mathcal{V} \times \mathcal{V} \rightarrow \mathbb{R}$ where $\mathcal{V} = \mathbb{R} \otimes_{\mathbb{Z}} L$. The *signature* of the bilinear form will always be given as a pair $(p, -q)$ where p denotes the number of positive and q the number of negative eigenvalues of the *Gram matrix* of Φ with respect to B which is denoted by ${}_B\Phi^B := (\Phi(b_i, b_j))_{i,j=1}^n$. By $L^\#$ we denote the *dual lattice* of L and in case that L is integral, i.e. $L \subseteq L^\#$, we write $\Delta(L) := L^\# / L$ for the *discriminant group* of L . The *automorphism group* of a lattice (L, Φ) is defined as

$$\text{Aut}(L) := \{g \in \text{GL}(\mathcal{V}) \mid Lg = L \text{ and } \Phi(xg, yg) = \Phi(x, y) \text{ for all } x, y \in L\}.$$

¹In the literature often referred to as a Lorentzian lattice

If (L, Φ) is an integral lattice, we can consider $\text{Aut}(L)$ as a subgroup of $\text{GL}_n(\mathbb{Z})$ by fixing a basis B of L :

$$\text{Aut}(L) \cong \text{Aut}_{\mathbb{Z}}(A) := \{g \in \text{GL}_n(\mathbb{Z}) \mid gAg^{tr} = A\},$$

where $A = {}_B\Phi^B$. Note that $\text{Aut}(L)$ acts on L from the right while it acts from the left on the set of Gram matrices of L .

For any ring R let $R^n := R^{1 \times n}$ the free R -module of rank n represented as a row vector. By e_i we denote the i th row of the $n \times n$ unit matrix I_n .

For a subset S of any R -module M let $\langle S \rangle_R$ submodule of M generated by S (mostly we will omit the subscript R if there are no confusions about the base ring to be worried about). Similarly, if S is a subset of some group G , we denote by $\langle S \rangle$ the subgroup of G generated by S .

2 Preliminaries

In this section we briefly recall the most important definitions and results from the first two sections of [13].

Throughout this section, let \mathcal{V} be a real vector space of dimension n and

$$\sigma : \mathcal{V} \times \mathcal{V} \rightarrow \mathbb{R}$$

be a positive definite bilinear form on \mathcal{V} .

Two non-empty open subsets $\mathcal{V}_1^{>0}, \mathcal{V}_2^{>0} \subset \mathcal{V}$ are called *dual cones* with respect to σ , if the following properties hold:

(DC.1) For $x \in \mathcal{V}_1^{>0}, y \in \mathcal{V}_2^{>0}$ we have $\sigma(x, y) > 0$.

(DC.2) If $\mathcal{V}_i^{\geq 0}$ denotes the topological closure of $\mathcal{V}_i^{>0}$ in \mathcal{V} then for any $x \in \mathcal{V} \setminus \mathcal{V}_1^{>0}$ there is a $y \in \mathcal{V}_2^{>0} \setminus \{0\}$ such that $\sigma(x, y) \leq 0$. The same holds for changed roles of x and y .

For fixed σ and dual cones $\mathcal{V}_1^{>0}, \mathcal{V}_2^{>0}$ a discrete subset $D \subset \mathcal{V}_2^{>0} \setminus \{0\}$ is called *admissible* if for every x in the boundary $\partial\mathcal{V}_1^{>0}$ of $\mathcal{V}_1^{>0}$ and every $\varepsilon > 0$ there is a $d \in D$ such that $\sigma(x, d) < \varepsilon$ (cf. [13, Definition 1.4, Lemma 1.5]). For such a set D and some vector $x \in \mathcal{V}_1^{>0}$ we define (cf. [13, Definition 1.2])

(i) The *D-minimum* of x :

$$\mu_D(x) := \min_{d \in D} \sigma(x, d),$$

(ii) The set of *D-minimal vectors* of x

$$M_D(x) = \{d \in D \mid \sigma(x, d) = \mu_D(x)\},$$

(iii) The *D-Voronoi domain* of x :

$$\mathcal{D}_D(x) := \left\{ \sum_{d \in M_D(x)} \alpha_d d \mid \alpha_d > 0 \right\}.$$

By [13, Lemma 1.1] this is all well-defined. Note that the set $M_D(x)$ is always finite, therefore $\mathcal{D}_D(x)$ is a pyramide in $\mathcal{V}_2^{\geq 0}$ based at the origin.

If the D -Voronoi domain of a vector $x \in \mathcal{V}_1^{>0}$ contains inner points, i.e. $\dim\langle M_D(x) \rangle = n$, then we call x a D -perfect vector. The set of all D -perfect vectors with D -minimum 1 shall be denoted by P_D (cf. [13, Definition 1.2]). As shown in [13, Proposition 1.8], P_D is not empty because for every $y \in \mathcal{V}_1^{>0}$ there exists some $x \in P_D$ such that $\mathcal{D}_D(y) \subseteq \mathcal{D}_D(x)$. The proof given there is constructive and can also be used to compute new D -perfect points from old ones.

Let $x \in P_D$. A vector $r \in \mathcal{V}_1 \setminus \{0\}$ with $\sigma(r, d) \geq 0$ for all $d \in M_D(x)$ and the additional property that $\sigma(r, d) = 0$ for $n - 1$ linearly independent vectors $d \in M_D(x)$ is called a *direction* of x . Every direction r of x defines a *facet* of the D -Voronoi domain $\mathcal{D}_D(x)$ by

$$\mathcal{F}(r) := \mathcal{D}_D(x) \cap \{y \in \mathcal{V}_2 \mid \sigma(r, y) = 0\}.$$

A direction that lies in $\mathcal{V}_1^{\geq 0}$ is called *blind*.

If r is a non-blind direction, then there exists a number $\rho > 0$ such that $y := x + \rho r \in P_D$. The D -perfect vector y is called a *neighbour* of x in direction r , the vectors x and y are called *contiguous*. Clearly for each D -perfect point there are (up to scaling) only finitely many directions, hence every $x \in P_D$ has finitely many neighbours.

By [13, Theorem 1.9], the D -Voronoi domains of the D -perfect points form a face-to-face tessellation of the whole cone $\mathcal{V}_2^{\geq 0}$, i.e. the (undirected) D -Voronoi graph Γ_D with vertex set P_D in which two vertices are adjacent if and only if the corresponding D -perfect points are contiguous, is connected and locally finite.

Now consider a group $\Omega \leq \text{GL}(\mathcal{V})$ which leaves the cone $\mathcal{V}_1^{>0}$ invariant and acts *properly discontinuously* on $\mathcal{V}_1^{>0}$, i.e. for $x \in \mathcal{V}_1^{>0}$

1. the orbit $x\Omega$ does not have a cluster point in $\mathcal{V}_1^{\geq 0}$ and
2. the stabilizer $\Omega_x := \text{Stab}_\Omega(x) := \{\omega \in \Omega \mid x\omega = x\}$ is finite.

For $\omega \in \Omega$ the *adjoint element* of ω is the unique $\omega^{ad} \in \text{GL}(\mathcal{V})$ fulfilling $\sigma(x\omega, y) = \sigma(x, y\omega^{ad})$ for all $x, y \in \mathcal{V}$. The *adjoint group* of Ω is defined by

$$\Omega^{ad} := \{\omega^{ad} \mid \omega \in \Omega\}.$$

By [13, Lemma 2.1], the group Ω acts on the D -Voronoi graph Γ_D in case that D is admissible.

There is a whole theory built around groups acting on graphs, often called Bass-Serre theory. We refer the reader to the monographs [5] by W. Dicks and [17] by J.-P. Serre for the original statement of the Bass-Serre theorem, which implies the following theorem if translated into this context.

Theorem 2.1. ([13, Theorem 2.2])

Let $\Omega \leq \text{GL}(\mathcal{V})$ act properly discontinuously on $\mathcal{V}_1^{>0}$ and let $D \subset \mathcal{V}_2^{\geq 0} \setminus \{0\}$ discrete, admissible and invariant under the action of Ω^{ad} . Furthermore, let X

denote a transversal of P_D/Ω such that the subgraph $\Gamma_D(X)$ of Γ_D generated by X is connected and put T as a maximal spanning tree of $\Gamma_D(X)$. The vertices of Γ_D which are adjacent to T are collected in the set $\delta(T)$. Finally, choose for $y \in \delta(T)$ one $\omega_y \in \Omega$ such that $y\omega_y^{-1} \in X$. Then it holds that

$$\Omega = \langle \omega_y, \text{Stab}_\Omega(x) \mid y \in \delta(T), x \in X \rangle.$$

In particular, Ω is finitely generated, if the residue class graph Γ_D/Ω is finite, i.e. there are only finitely many D -perfect points up to action of Ω .

In case that the residue class graph is finite, the above theorem immediately gives a template algorithm to compute a generating system for Ω :

Algorithm 2.2.

Input: $\mathcal{V}_1^{>0}, \mathcal{V}_2^{>0}$ dual cones w.r.t. σ , $D \subset \mathcal{V}_2^{>0} \setminus \{0\}$ discrete, admissible and Ω -invariant.

Output: a transversal for P_D/Ω , generators for Ω .

1. Find a D -perfect point x_1 and initialize $L_1 = \{x_1\}$, $L_2 := \emptyset$, $S := \emptyset$.
2. If $L_1 = \emptyset$, then return L_2, S ; else choose $x \in L_1$.
3. Compute a generating system S_x for Ω_x and put $S := S \cup S_x$.
4. Compute the set R of neighbours of x and a transversal R' of R/Ω_x .
5. For $y \in R'$ decide whether there is a $z \in L_1 \cup L_2$ and an $\omega \in \Omega$ with $y\omega = z$.
If not, put $L_1 := L_1 \cup \{y\}$.
If $z \in L_1$ then put $S := S \cup \{\omega\}$.
6. Put $L_2 := L_2 \cup \{x\}$, $L_1 := L_1 \setminus \{x\}$. Go to step 2.

One of the crucial problems using the above method is to prove the finiteness of the residue class graph Γ_D/Ω . For Opgenorth's normalizer algorithm this was proven in [6] and [12]. In general there is the following theorem which is a generalization of [8, Satz 6].

Theorem 2.3. (Koecher, 1960)

Let L a full lattice in \mathcal{V} and $D \subseteq \mathcal{V}_2^{>0} \cap L \setminus \{0\}$ admissible. Assume that $L\Omega^{ad} = L$ and $D\Omega^{ad} = D$. Then the following are equivalent:

- (1) There are only finitely many Ω -equivalence classes of D -perfect points with D -minimum 1.
- (2) There exists a set $\tilde{\mathbb{F}} \subset \mathcal{V}_2^{>0}$ fulfilling that for every $y \in \mathcal{V}_2^{>0}$ there is an $\omega \in \Omega$ such that $x\omega \in \tilde{\mathbb{F}}$, such that there is a $y_0 \in \mathcal{V}_2^{>0}$ with $d - y_0 \in \mathcal{V}_2^{>0}$ for all $d \in \tilde{\mathbb{F}} \cap L$.

Koecher only proves the direction (1) \Rightarrow (2) of the equivalence for self-dual cones, but his proof works with some straight forward modifications for dual cones as well. The other direction follows immediately from an assertion (cf. [8, p.400]) of which Koecher's proof can also be easily adapted.

The condition (2) in Theorem 2.3 is fulfilled for example if there is a finite set $M \subset D$ such that the pyramide $P(M) = \{\sum_{d \in M} \alpha_d d \mid \alpha_d \geq 0\}$ contains a fundamental domain for the action of Ω^{ad} (cf. [13, Proposition 2.5]).

3 Hyperbolic Lattices

In this section we are going to give detailed and explicit methods how to apply Algorithm 2.2 to compute generators for the automorphism group of a hyperbolic lattice. For this purpose, we first have to find a pair of dual cones with respect to a bilinear form.

Throughout this section, we consider integral lattices (L, Φ) where Φ is a bilinear form of signature $(n-1, -1)$. We also assume that there is a fixed basis B of L and we set $A := {}_B \Phi^B \in \mathbb{Z}^{n \times n}$. The set of real (integral) hyperbolic matrices is denoted by $\mathbb{R}_{hyp}^{n \times n}$ ($\mathbb{Z}_{hyp}^{n \times n}$).

With respect to this basis, we identify $\mathcal{V} := \mathbb{R} \otimes_{\mathbb{Z}} L \cong \mathbb{R}^n$. Therefore we will not always distinguish strictly between the lattice (L, Φ) and its Gram matrix A .

3.1 Hyperbolic Lattices and Dual Cones

Lemma 3.1.

Consider the standard hyperbolic matrix

$$H := \text{diag}(-1, 1, \dots, 1) \in \mathbb{Z}_{hyp}^{n \times n}.$$

Then the set

$$\mathcal{C} := \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid xHx^{tr} < 0 \text{ and } x_1 > 0\} \quad (1)$$

is a selfdual cone with respect to the standard scalar product.

Proof. Obviously, \mathcal{C} is an open, nonempty set.

To prove the property (DC.1), let $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathcal{C}$. Without loss of generality, we may assume that $x_1 = y_1$, since we can rescale y by a positive real number. We calculate

$$\begin{aligned} xy^{tr} &= x_1 y_1 + \sum_{i=2}^n x_i y_i \\ &= \frac{1}{2}(x_1^2 + y_1^2) + \sum_{i=2}^n \frac{1}{2}((x_i + y_i)^2 - x_i^2 - y_i^2) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2} \left((x_1^2 - \sum_{i=2}^n x_i^2) + (y_1^2 - \sum_{i=2}^n y_i^2) + \sum_{i=2}^n (x_i - y_i)^2 \right) \\
&= \frac{1}{2} \left(\underbrace{-xHx^{tr}}_{>0} + \underbrace{(-yHy^{tr})}_{>0} + \underbrace{\sum_{i=2}^n (x_i - y_i)^2}_{\geq 0} \right) > 0
\end{aligned}$$

hence (DC.1) is shown.

Regarding (DC.2) let $x = (x_1, \dots, x_n) \notin \mathcal{C}$. If $x_1 \leq 0$, the $y = (1, 0, \dots, 0) \in \mathcal{C}$ fulfills $xy^{tr} = x_1 \leq 0$. Thus suppose $x_1 > 0$. By definition of \mathcal{C} we know that $-x_1^2 + s \geq 0$ for $s := \sum_{i=2}^n x_i^2$, hence especially $s > 0$. As above we may therefore assume $s = 1$. This yields $0 < x_1^2 \leq 1$. Now define $y = (1, -x_2, \dots, -x_n)$. It holds $yHy^{tr} = 0$ and $y_1 = 1 > 0$, thus $y \in \bar{\mathcal{C}}$ and $xy^{tr} = x_1 - 1 \leq 0$ as desired. \square

We remark here that for dual cones $\mathcal{V}_1^{>0}, \mathcal{V}_2^{>0}$ with respect to a bilinear form σ the sets $\mathcal{V}_1^{>0}g$ and $\mathcal{V}_2^{>0}(g^{ad})^{-1}$ are dual cones with respect to σ for every $g \in \text{GL}(\mathcal{V})$.

Now Sylvester's Law of Inertia states that for any $A \in \mathbb{R}_{hyp}^{n \times n}$ there is a $T \in \text{GL}_n(\mathbb{R})$ such that $TAT^{tr} = H$. Thus we obtain that for any such T

$$\mathcal{V}_1^{>0} := \mathcal{C}T^{-1} = \{x \in \mathbb{R}^n \mid xAx^{tr} < 0 \text{ and } xy_1^{tr} > 0\} \quad (2)$$

$$\mathcal{V}_2^{>0} := \mathcal{C}T^{tr} = \{x \in \mathbb{R}^n \mid xA^{-1}x^{tr} < 0 \text{ and } xy_2^{tr} > 0\}, \quad (3)$$

where $y_1 = e_1T^{-1}$ and $y_2 = e_1T^{tr}$, are dual cones with respect to the standard scalar product.

Remark 3.2.

Note that the dual cones $\mathcal{V}_1^{>0}$ and $\mathcal{V}_2^{>0}$ in (2) and (3) depend on the choice of T , but the second output of Algorithm 2.2 being a generating system for the group Ω does not depend on the choice of the dual cones, as long as Ω acts on them.

In fact $\Omega = \text{Aut}_{\mathbb{Z}}(A)$ does not act on $\mathcal{V}_1^{>0}$ because one has $-I_n \in \text{Aut}_{\mathbb{Z}}(A)$ for all symmetric matrices A but certainly $\mathcal{V}_1^{>0} \neq \mathcal{V}_1^{>0}(-I_n)$. But $\text{Aut}_{\mathbb{Z}}(A)$ acts on $\mathcal{V}_1^{>0} \cup (-\mathcal{V}_1^{>0})$ and thus we can restrict ourselves to the stabilizer of $\mathcal{V}_1^{>0}$ in $\text{Aut}_{\mathbb{Z}}(A)$ which from now on will be denoted by Ω . We shall call Ω the reduced automorphism group of A or L respectively. Obviously we have $\text{Aut}_{\mathbb{Z}}(A) = \Omega \times \langle -I_n \rangle$.

Lemma 3.3.

The group Ω acts properly discontinuously on $\mathcal{V}_1^{>0}$.

Proof. Suppose that there is a cluster point x^* of the orbit $x\Omega$ of some $x \in \mathcal{V}_1^{>0}$. Then there is a sequence $(\omega_k)_{k \in \mathbb{N}}$ in Ω such that $x\omega_k$ tends to x^* as k tends to ∞ . Obviously we have $xAx^{tr} = (x\omega_k)A(x\omega_k)^{tr}$ for all k , hence also $x^*Ax^{tr} = xAx^{tr}$. Since the real automorphism group modulo $-I_n$ denoted $\Omega_{\mathbb{R}}$ acts transitively on the set $\{x \in \mathcal{V}_1^{>0} \mid xAx^{tr} = c\}$ for any given number

$c > 0$, there must be an $\omega^* \in \Omega_{\mathbb{R}}$ such that $x\omega^* = x^*$. By choosing the right representatives modulo $\text{Stab}_{\Omega_{\mathbb{R}}}(x^*)$ we may assume that $\omega_k \rightarrow \omega^*$, but because Ω is discrete this means that the sequence $(\omega_k)_{k \in \mathbb{N}}$ and hence the sequence $(x\omega_k)_{k \in \mathbb{N}}$ becomes constant at some point.

As will be shown in Lemma 3.12, the stabilizer of any $x \in \mathcal{V}_1^{>0}$ is isomorphic to a subgroup of the automorphism group of a positive definite lattice, thus it must be finite.

Therefore the action of Ω on $\mathcal{V}_1^{>0}$ is properly discontinuous. \square

3.2 Admissibility

For the rest of this paper let

$$D := \mathbb{Z}^n \cap \mathcal{V}_2^{\geq 0} \setminus \{0\}. \quad (4)$$

This set is obviously discrete and Ω^{ad} -invariant. In this subsection we want to prove that D is admissible, which is less obvious.

Remark 3.4.

For every $\varepsilon > 0$ and $x \in \mathbb{R}^n$ the set

$$P_\varepsilon(x) := \{y \in \mathbb{R}^n \mid 0 \leq xy^{tr} \leq \varepsilon\}$$

contains a point $\neq 0$ with integral coordinates.

Proof. For given $\varepsilon > 0$ and $x \in \mathbb{R}^n$ consider

$$X := \{y \in \mathbb{R}^n \mid -\varepsilon \leq xy^{tr} \leq \varepsilon\}.$$

This set is clearly centrally symmetric and convex and has infinite volume. Thus by Minkowski's Convex Body Theorem ([11, Satz 4.4]) we know that $X \cap \mathbb{Z}^n \neq \{0\}$. For $\ell \in X \cap \mathbb{Z}^n \setminus \{0\}$ we either have $x\ell^{tr} \geq 0$ and thus $\ell \in P_\varepsilon(x)$ or $x\ell^{tr} \leq 0$ and thus $-\ell \in P_\varepsilon(x)$. \square

In addition we will need a famous result by Lovász. To understand it we need the following definition (cf. [2]).

Definition 3.5.

(i) Let $S \subseteq \mathbb{R}^n$ convex. We call S a maximal lattice-free convex set, for short MLFC-set, if it holds that

(a) the relative interior of S with respect to $\langle S \rangle_{\mathbb{R}}$ does not contain points with integral coordinates,

(b) S is maximal (with respect to inclusion) among all convex subsets $T \subseteq \mathbb{R}^n$ fulfilling property (a).

(ii) Let \mathcal{U} an affine subspace of \mathbb{R}^n . If the integral points in \mathcal{U} generate \mathcal{U} as an affine space, i.e.

$$\langle \mathcal{U} \cap \mathbb{Z}^n \rangle_{aff} = \mathcal{U},$$

then we call \mathcal{U} a rational subspace of \mathbb{R}^n . If not, \mathcal{U} is called irrational.

Theorem 3.6. (Lovász, 1989)

Let $S \subseteq \mathbb{R}^n$. It holds that S is an MCLF-set if and only if one of the following conditions hold:

1. S is a convex polyhedron of the form $S = P + \mathcal{L}$, where P is a polytope and \mathcal{L} is a rational vector space, whereby it holds that $\dim \langle P \rangle + \dim \mathcal{L} = n$ and $S^\circ \cap \mathbb{Z}^n = \emptyset$ and every surface of S contains an integral point in its relative interior.
2. S is an irrational affine hyperplane of \mathbb{R}^n of dimension $n - 1$.

A proof of this can be found in [2].

Remark 3.7.

Let $S = P + \mathcal{L}$ an MCLF-set as in Theorem 3.6,1. Then P must be a bounded polytope since the surfaces of S contain an integral point in their relative interior. By adding suiting integral points if necessary one gets a basis of a full-rank sublattice of \mathbb{Z}^n which has a fundamental polytope F . The projection of F onto $\langle P \rangle$ must be contained properly in P if P is unbounded which yields a contradiction to S being lattice-free.

We can now prove the following:

Proposition 3.8.

The set D from equation (4) is admissible.

Proof. Let $x \in \partial \mathcal{V}_1^{>0}$. By [13, Lemma 1.1] there is a $y \in \mathcal{V}_2^{>0} \setminus \{0\}$ such that $xy^{tr} = 0$. Now let $\varepsilon > 0$ and define

$$M_\varepsilon := \{v \in \mathcal{V}_2^{>0} \setminus \{0\} \mid xv^{tr} \leq \varepsilon\}.$$

We have to show that $M_\varepsilon \cap D \neq \emptyset$.

Assume on the contrary that this were false. Then, since M_ε is convex, there must be an MCLF-set $S \subset \mathbb{R}^n$ with $M_\varepsilon \subseteq S$. Obviously, S cannot be an affine hyperplane, hence $S = P + \mathcal{L}$ as in Theorem 3.6,1. Since P is bounded, it can't hold that $y \in P$, thus $y = p + \ell$ for some $p \in P$, $\ell \in \mathcal{L} \setminus \{0\}$. For reasons of dimension, p and ℓ are in fact unique. Now let $\lambda > 0$. Thus $\lambda y = \lambda p + \lambda \ell$, but since P is bounded and $\lambda y \in M_\varepsilon \subseteq S = P + \mathcal{L}$, this cannot hold for big values of λ if $p \neq 0$. Thus $y \in \mathcal{L}$.

Now consider for $0 \leq \varepsilon' \leq \varepsilon$ the set

$$T_{\varepsilon'}(x) := \{v \in \mathbb{R}^n \mid xv^{tr} = \varepsilon'\}.$$

Then for each such ε' we can find some $v_{\varepsilon'} \in \mathcal{V}_2^{>0} \cap T_{\varepsilon'}(x)$, hence we can write

$$T_{\varepsilon'}(x) = v_{\varepsilon'} + T_0(x)$$

and thus

$$P_\varepsilon = \bigcup_{0 \leq \varepsilon' \leq \varepsilon} (v_{\varepsilon'} + T_0(x)).$$

For fixed $0 \leq \varepsilon' \leq \varepsilon$ let $v_{\varepsilon'} = p' + \ell'$ where $p \in P$ and $\ell \in \mathcal{L}$. Now for every $y \in T_0(x)$, there is some $\lambda_0 > 0$ such that

$$v_{\varepsilon'} + \lambda y \in \mathcal{V}_2^{\geq 0} \text{ for all } \lambda \geq \lambda_0.$$

We can decompose $v_{\varepsilon'} + \lambda_0 y = p + \ell$ with $p \in P$, $\ell \in \mathcal{L}$, thus we have

$$\lambda_0 y = (p - p') + (\ell - \ell').$$

For $\lambda \geq \lambda_0$ this implies that

$$v_{\varepsilon'} + \lambda y = \underbrace{p' + \frac{\lambda}{\lambda_0}(p - p')}_{\in P} + \underbrace{\ell' + \frac{\lambda}{\lambda_0}(\ell - \ell')}_{\in \mathcal{L}}$$

which can only hold if $p = p'$ because P is bounded. But this means that $y \in \mathcal{L}$ and hence it follows $v_{\varepsilon'} + T_0(x) \subseteq P + \mathcal{L}$ for all ε' , and therefore $P_\varepsilon(x) \subseteq S$ which is a contradiction to Remark 3.4. \square

3.3 D -Minimal Vectors and Automorphisms

Now that we have found the dual cones and an admissible set D , we give explicit methods to calculate the D -minimal vectors of a point $x \in \mathcal{V}_1^{>0}$ as well as its stabilizer and connecting elements.

As stated before, we consider $A \in \mathbb{Z}_{hyp}^{n \times n}$ a given hyperbolic matrix with a fixed pair of dual cones $\mathcal{V}_1^{>0}, \mathcal{V}_2^{>0}$ and cone test vectors y_1, y_2 as in equations (2) and (3) and D as in equation (4).

Remark 3.9.

(i) For any $x \in \mathcal{V}_1^{>0}$, it holds that $-xA \in \mathcal{V}_2^{>0}$.

(ii) Let $x \in \mathcal{V}_1^{>0} \cap \mathbb{Z}^n$. Then we have $\mu_D(x) \leq -xAx^{tr} =: N(x)$.

Proof. (i) is clear for $A = H$ with $H = \text{diag}(-1, 1, \dots, 1)$ and in general follows from Sylvester's Law of Inertia.

(ii) follows from (i) because $-xA \in D$ and thus $\mu_D(x) \leq x(-xA)^{tr} = -xAx^{tr}$. \square

Lemma 3.10.

Let $x \in \mathcal{V}_1^{>0} \cap \mathbb{Z}^n$ and $\lambda > 0$ and define the affine hyperplane

$$H_\lambda(x) := \{-\lambda xA + y \in \mathbb{R}^n \mid xy^{tr} = 0\}.$$

If λ is minimal such that the finite set

$$M_\lambda = \{d \in H_\lambda(x) \cap \mathbb{Z}^n \mid (d + \lambda xA)A^{-1}(d + \lambda xA)^{tr} \leq \lambda^2 xAx^{tr} \text{ and } y_2 d^{tr} \geq 0\}$$

is nonempty, it holds that

$$M_\lambda = M_D(x).$$

Proof. First of all we note that there actually is a minimal λ such that $M_\lambda \neq \emptyset$. For that let $d = -\lambda xA + y \in H_\lambda(x) \cap \mathbb{Z}^n$. Since by assumption $x \in \mathbb{Z}^n$ and $A \in \mathbb{Z}_{hyp}^{n \times n}$ it holds that

$$xd^{tr} = -\lambda \underbrace{xAx^{tr}}_{\in \mathbb{Z}} + \underbrace{xy^{tr}}_{=0} = \lambda N(x) \in \mathbb{Z},$$

thus it follows that for M_λ to be nonempty it is necessary that $\lambda \in \frac{1}{N(x)}\mathbb{Z}$.

We calculate

$$dA^{-1}d^{tr} = -\lambda^2 N(x) + yA^{-1}y^{tr},$$

thus minimizing λ means minimizing xd^{tr} .

For d to belong to $\mathcal{V}_2^{\geq 0}$ it is further necessary that

$$(d + \lambda xA)A^{-1}(d + \lambda xA)^{tr} \leq \lambda^2 N(x),$$

and thus we get that $M_\lambda \subseteq D$, and hence $M_\lambda = M_D(x)$ for the minimal λ with $M_\lambda \neq \emptyset$. \square

Remark 3.11.

There are algorithms to calculate short vectors in positive definite lattices, see for instance [16, pp. 188-190]. We can use them to calculate the set M_λ for $\lambda = \frac{1}{N(x)}, \frac{2}{N(x)}, \dots$ until M_λ is not empty in the following way:

The matrix A^{-1} induces a positive definite scalar product on the subspace $H_0(x)$ of \mathbb{R}^n . We can thus calculate all $y \in H_0(x)$ such that $d = -\lambda xA + y \in \mathbb{Z}^n$, which especially means that y is contained in the lattice $\frac{1}{N(x)}\mathbb{Z}^n \cap H_0(x)$ endowed with the bilinear form induced by A^{-1} , and

$$yA^{-1}y^{tr} \leq \lambda^2 N(x).$$

Since $-xA \in H_1(x)$ is an integral point, we have to repeat this at most $N(x)$ times.

Lemma 3.12.

- (i) *Since A is an integral matrix, all D -perfect vectors have integer entries (up to scaling). Thus we can restrict ourselves on integral vectors x .*
- (ii) *Let x an integral D -perfect point and $g \in S_x := \text{Stab}_\Omega(x)$. Then g induces an automorphism of the positive definite lattice $L(x) = H_0(xA) \cap \mathbb{Z}^n$ with scalar product induced by A .*

Proof. (i) is clear.

Regarding (ii), we have that $x \in \mathcal{V}_1^{\geq 0}$ and thus $xAx^{tr} < 0$. In addition it is perpendicular with respect to the bilinear form induced by A to $L(x)$, hence this bilinear form must be positive definite on the orthogonal complement $H_0(xA)$ of x . That g induces an automorphism of $L(x)$ is easily calculated. \square

Remark 3.13.

- (i) There are quite powerful methods to calculate the automorphism group of a positive definite lattice, see for instance [15]. Thus we can calculate the automorphisms of $L(x)$ and continue them such that they act trivially on x . This can be done by adding x to a lattice basis of $L(x)$ to obtain a basis of \mathbb{R}^n . With respect to this basis, the automorphisms have the form

$$\left(\begin{array}{c|c} g & 0 \\ \hline 0 & 1 \end{array} \right), \quad g \in \text{Aut}(L(x)).$$

Changing the basis to B chosen in the very beginning yields a subgroup G_x of rational automorphisms of A . The elements in G_x that fix \mathbb{Z}^n as a point set are exactly the elements in S_x .

- (ii) A slight modification of this also gives a method to determine the connecting elements in Theorem 2.1. For D -perfect vectors $x, y \in \mathcal{V}_1^{>0}$ with $N(x) = N(y)$ we calculate integral isometries of the lattices $L(x) \rightarrow L(y)$. If there are no isometries, then x and y are inequivalent under Ω , if there are then continuing them onto all of \mathbb{R}^n such that $x \mapsto y$ yields again some rational automorphisms of A , of which it is to determine, whether it is integral or not. If there is an integral one, this yields such a connecting element denoted ω_y in Theorem 2.1. If not, then again, x and y are not equivalent under Ω .

Note that this last case does in fact occur.

3.4 Finiteness of the Residue Class Graph

Up until now, we have given explicit methods to solve all the computational tasks in the algorithm in section 2. But it is not clear at all, that Algorithm 2.2 terminates for any integral hyperbolic lattice, i.e. for the reduced automorphism group of any such lattice there is only a finite number of inequivalent perfect points. In this subsection we will prove this using similar methods as in [18], where C.L. Siegel has proven that the automorphism group of any definite or indefinite lattice is finitely generated.

We recall some of Siegel's results. For that let $S \in \mathbb{Z}^{n \times n}$ be an integral symmetric matrix of signature $(m, -(n-m))$ and Ω its reduced automorphism group. Consider the equation

$$HS^{-1}H = S \tag{5}$$

for positive definite matrices $H \in \mathbb{R}_{>0}^{n \times n}$. The solutions of equation (5) form a rational manifold \mathfrak{H} of dimension $m(n-m)$ which can be parametrized by

$$H = 2Z - S, \quad Z = \left(\begin{array}{c|c} T^{-1} & T^{-1}Y^{tr} \\ \hline YT^{-1} & YT^{-1}Y^{tr} \end{array} \right), \quad T = (I_m \mid Y^{tr})S^{-1} \left(\begin{array}{c} I_m \\ Y \end{array} \right), \tag{6}$$

where where $Y \in \mathbb{R}^{(n-m) \times m}$ is chosen such that T is positive definite (see [18, Equation (35)]). Note that Ω acts from the left on \mathfrak{H} by

$$(g, H) \mapsto gHg^{tr}$$

and from the right on the corresponding set of Y by

$$(Y, g) \mapsto g^{tr} \left(\frac{I_m}{Y} \right)$$

where we have to renormalize the last term (by multiplication with a matrix $Q \in \text{GL}_m(\mathbb{R})$) such that the upper part becomes again I_m . Thus we get a rational injection

$$\phi : \mathfrak{H} \rightarrow \mathbb{R}^{(n-m) \times m}, H \mapsto Y \quad (7)$$

which is Ω -equivariant.

Using reduction theory of quadratic forms due to H. Minkowski and results by C. Hermite, Siegel constructs a fundamental domain \mathbb{F} of Ω in \mathfrak{H} .

Theorem 3.14. (*Siegel, 1940*)

Let $S \in \mathbb{Z}^{n \times n}$ be an integral symmetric matrix of signature $(m, -(n-m))$. There is a finite number of hyperplanes in the subspace of $\mathbb{R}_{sym}^{n \times n}$ spanned by \mathfrak{H} such that \mathbb{F} is an intersection of the corresponding halfspaces and the manifold \mathfrak{H} of all matrices H fulfilling equation (5). In addition, \mathbb{F} has only finitely many neighbours, that means there are only finitely many elements $\omega \in \Omega$ with $\mathbb{F} \cap \mathbb{F}\omega \neq \emptyset$.

Proof. [18, Satz 10] □

Equipped with these results we can now prove the main result of this subsection.

Theorem 3.15. Let $A \in \mathbb{Z}_{hyp}^{n \times n}$ be an integral hyperbolic matrix, Ω its reduced automorphism group and $\mathcal{V}_i^{>0}$ and D as in equations (2)-(4). Then the residue class graph Γ_D/Ω is finite. In particular, Algorithm 2.2 terminates.

Proof. Obviously, we can replace A by $-A$ without changing Ω . Especially it holds that $x(-A)^{-1}x^{tr} > 0$ for every $x \in \mathcal{V}_2^{>0}$. The signature of $-A$ is $(1, 1-n)$, thus the manifold \mathfrak{H} as described in equation (6) is homeomorphic via ϕ in equation (7) to the manifold $\mathcal{V}_2^{>0}/\mathbb{R}_{>0}$ as we can rescale each cone vector such that its first coordinate is 1. Since ϕ is Ω -equivariant, the fundamental domain \mathbb{F} is mapped to a fundamental domain $\tilde{\mathbb{F}} \subset \mathcal{V}_2^{>0}$ of the action of Ω . Theorem 3.14 tells us that \mathbb{F} and therefore $\tilde{\mathbb{F}}$ are bounded by finitely many hyperplanes in \mathbb{R}^n . But then Theorem 2.3 implies that there are only finitely many D -perfect points modulo Ω , hence the assertion follows. □

Remark 3.16. Since Theorem 3.14 is not restricted to a certain signature of the matrix S , it is very likely that the method described here will yield a more

general procedure to determine the automorphism group of any indefinite lattice. In that case one would have to define the dual cones as subsets of $\mathbb{R}^{n \times m}$ in an analogous way, replacing the symbols $<$ and $>$ by "negative" and "positive definite" respectively.

3.5 The Watson-Process

In this subsection we are going to recall the Watson process, that enables us to reduce the discriminant of a quadratic form without increasing its class number. See e.g. [21] and [9] for details. For that purpose, consider for a moment (L, Φ) to be an integral lattice with a symmetric, non-degenerate bilinear form Φ of arbitrary signature.

Definition 3.17.

Let p a prime number such that $\Delta(L)$ contains an element of order p^2 . The integral lattice

$$\text{Fill}_p(L) := (pL^\# \cap L, \frac{1}{p}\Phi)$$

is called a p -filling of L .

The p -filling has the following effect on the genus symbol of L in the sense of [4, Chapter 15]: For the p -filling to be defined, the highest level of a p -adic Jordan constituent of L must be at least 2. The p -filling reduces this level by 2. Repeating this until it is no longer possible yields the so called *Watson lattice* of L , denoted by $\text{Watson}(L)$. The mapping $L \mapsto \text{Watson}(L)$ is called the *Watson process*.

Remark 3.18.

For an integral lattice L , the discriminant group $\Delta(\text{Watson}(L))$ has squarefree exponent by construction and, which is even more important for computational issues, the discriminant $|\Delta(L)|$ is decreased by the Watson process by a factor p^2 for every p -filling during the Watson process.

Remark 3.19.

Since p -filling (and therefore the Watson process) cannot be expressed as an action of $\text{GL}_n(\mathbb{Z})$, the automorphism groups of L and $\text{Fill}_p(L)$ will not be isomorphic. But up to isomorphism one always has

$$\text{Aut}(L) \leq \text{Aut}(\text{Fill}_p(L)) \quad \text{and} \quad [\text{Aut}(\text{Fill}_p(L)) : \text{Aut}(L)] < \infty.$$

Hence one can determine $\text{Aut}(L)$ again via an orbit-stabilizer computation in $\text{Aut}(\text{Fill}_p(L))$ or $\text{Aut}(\text{Watson}(L))$ respectively.

Although we cannot prove it, so far all examples suggest that first calculating $\text{Aut}_{\mathbb{Z}}(\text{Watson}(A))^2$ via the algorithm and then finding $\text{Aut}_{\mathbb{Z}}(A)$ as a co-finite subgroup in it via an orbit-stabilizer calculation makes the computation very much faster, provided that the Watson process has any effect.

²We use the same notation for the Gram matrices of the lattices involved

Heuristically, this could be explained by two observations: Since the automorphism group of $\text{Watson}(L)$ properly contains the one of L up to isomorphism, thus the corresponding equivalence relation on the set of D -perfect points is in a way coarser for $\text{Watson}(L)$ than for L . Thus one can expect that modulo $\text{Aut}(\text{Watson}(L))$ there will be fewer classes of D -perfect points than modulo $\text{Aut}(L)$.

Furthermore, the computation time to determine D -minimal vectors of $x \in \mathcal{V}_1^{>0} \cap \mathbb{Z}^n$ depends among others on the discriminant of the lattice $(\frac{1}{N(x)}\mathbb{Z}^n \cap H_0(x), A^{-1})$ and the number $N(x)$. Both numbers tend to be smaller for $\text{Watson}(L)$ than for L . Since in most cases one has to calculate D -minimal vectors for many different vectors x , an acceleration of the computation of D -minimal vectors is quite valuable.

The strength of this slight modification is illustrated in Example 4.2.

4 Examples

All computations were executed on a Quad-Core AMD Opteron(tm) Processor 8356 running at 1150 GHz. The used MAGMA version is V2.19-1.

Throughout this section we consider the lattice (\mathbb{Z}^n, Φ) where the Gram matrix of Φ with respect to the standard basis is given by A .

Example 4.1.

Our first example we discuss the steps of the algorithm in detail. We take here

$$A = \begin{pmatrix} -1 & -3 & -1 \\ -3 & 14 & 8 \\ -1 & 8 & 11 \end{pmatrix}, \quad A^{-1} = \frac{1}{155} \begin{pmatrix} -90 & -25 & 10 \\ -25 & 12 & -11 \\ 10 & -11 & 23 \end{pmatrix}.$$

For this matrix the algorithm finds 9 inequivalent D -perfect points. Rescaled such that their entries become integral, they are represented by

$$\begin{aligned} x_1 &= (1 & 0 & 0) & x_2 &= (2 & 1 & -1) & x_3 &= (2 & 1 & 0) \\ x_4 &= (9 & 0 & -2) & x_5 &= (5 & 3 & -3) & x_6 &= (12 & 5 & -7) \\ x_7 &= (3 & 2 & -1) & x_8 &= (14 & 9 & -2) & x_9 &= (21 & 8 & -12) \end{aligned}$$

where these points each have got (in the listed order) 8, 4, 6, 8, 4, 3, 4, 3 and 6 neighbours. The stabilizers of x_2, x_5, x_6, x_7, x_8 are trivial and all the other stabilizers are cyclic of order 2 given by

$$\begin{aligned} \text{Stab}(x_1) &= \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 6 & -1 & 0 \\ 2 & 0 & -1 \end{pmatrix} \right\rangle & \text{Stab}(x_3) &= \left\langle \begin{pmatrix} 9 & 5 & 0 \\ -16 & -9 & 0 \\ -12 & -6 & -1 \end{pmatrix} \right\rangle \\ \text{Stab}(x_4) &= \left\langle \begin{pmatrix} 125 & 0 & -28 \\ 774 & -1 & -172 \\ 558 & 0 & -125 \end{pmatrix} \right\rangle & \text{Stab}(x_9) &= \left\langle \begin{pmatrix} 1385 & 528 & -792 \\ 1974 & 751 & -1128 \\ 3738 & 1424 & -2137 \end{pmatrix} \right\rangle \end{aligned}$$

In addition, we find 16 connecting elements

$$\begin{aligned}
c_{1,1} &= \begin{pmatrix} 31 & -5 & 10 \\ 96 & -15 & 32 \\ -48 & 8 & -15 \end{pmatrix} & c_{4,1} &= \begin{pmatrix} 125 & 0 & -28 \\ -24 & 1 & 4 \\ -308 & 0 & 69 \end{pmatrix} \\
c_{4,4} &= \begin{pmatrix} 561 & -28 & -84 \\ 3920 & -195 & -588 \\ 2440 & -122 & -365 \end{pmatrix} & c'_{4,4} &= \begin{pmatrix} 145 & 9 & -44 \\ 966 & 59 & -292 \\ 642 & 40 & -195 \end{pmatrix} \\
c_{4,8} &= \begin{pmatrix} 1005 & 5 & -232 \\ -1784 & -9 & 412 \\ -1048 & -6 & 243 \end{pmatrix} & c_{5,5} &= \begin{pmatrix} 289 & 180 & -180 \\ -96 & -59 & 60 \\ 368 & 230 & -229 \end{pmatrix} \\
c'_{5,5} &= \begin{pmatrix} 51 & 35 & -30 \\ -40 & -27 & 24 \\ 40 & 28 & -23 \end{pmatrix} & c_{5,8} &= \begin{pmatrix} 109 & 57 & -68 \\ -186 & -97 & 116 \\ -82 & -42 & 51 \end{pmatrix} \\
c_{6,6} &= \begin{pmatrix} 139 & 63 & -84 \\ 120 & 53 & -72 \\ 320 & 144 & -193 \end{pmatrix} & c_{7,9} &= \begin{pmatrix} 591 & 432 & -224 \\ 880 & 643 & -332 \\ 1620 & 1184 & -613 \end{pmatrix} \\
c_{7,7} &= \begin{pmatrix} 45 & 33 & -22 \\ -56 & -41 & 28 \\ 8 & 6 & -3 \end{pmatrix} & c_{8,5} &= \begin{pmatrix} 75 & 51 & -16 \\ 26 & 17 & -4 \\ 142 & 96 & -29 \end{pmatrix} \\
c_{8,4} &= \begin{pmatrix} 9 & 5 & 0 \\ 70 & 39 & 0 \\ 30 & 16 & 1 \end{pmatrix} & c_{9,7} &= \begin{pmatrix} 231 & 96 & -136 \\ -374 & -155 & 220 \\ -118 & -48 & 69 \end{pmatrix} \\
c_{9,9} &= \begin{pmatrix} 1575 & 603 & -902 \\ 2506 & 961 & -1436 \\ 4422 & 1694 & -2533 \end{pmatrix} & c_{9,6} &= \begin{pmatrix} 1385 & 528 & -792 \\ 1974 & 751 & -1128 \\ 3738 & 1424 & -2137 \end{pmatrix}.
\end{aligned}$$

The notation shall be understood that via the connecting element $c_{i,j}$ the D -perfect points x_i and x_j are adjacent in the residue class graph, in other words x_i and $x_j c_{i,j}^{-1}$ are contiguous. The precise contiguity relations between the points are represented in the residue class graph Γ_D/Ω . The straight lines represent direct contiguity, the curved ones contiguity by the connecting elements which are labeled on the edges.

Calculating this information takes about 4.4 seconds.

In the first example it does not matter whether one applies the Watson process since it does not have any effect on the matrix and runs in virtually no time. The following example shall illustrate the situation when the Watson process does change things.

Example 4.2.

In this example we want to demonstrate how effective the usage of the Watson

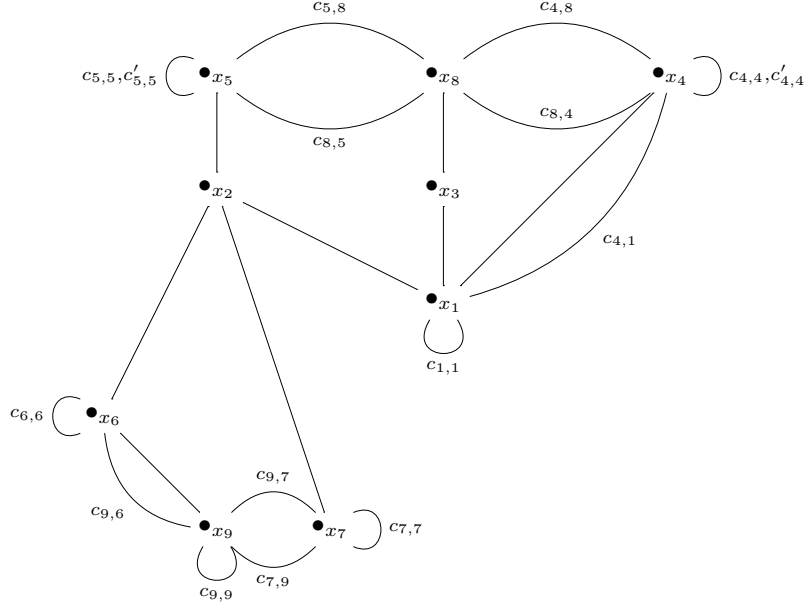


Figure 1: Residue class graph Γ_D/Ω

process can be. For that purpose, we look at the matrix

$$A = \begin{pmatrix} 9 & -2 & 7 \\ -2 & -2 & 8 \\ 7 & 8 & 9 \end{pmatrix}, \quad A^{-1} = \frac{1}{450} \begin{pmatrix} 41 & -37 & 1 \\ -37 & -16 & 43 \\ 1 & 43 & 11 \end{pmatrix}.$$

We have $\det A = -2^2 \cdot 3^2 \cdot 5^2$ and the genus symbol (in the notation of [4], neglecting the additional parameters of the 2-adic genus symbol) of A is given by

$$(1 \cdot 2^2)(1^{-1} \cdot 9)(1^{-2} \cdot 25^{-1}),$$

thus the Watson process does have an effect and yields

$$\text{Watson}(A) = \begin{pmatrix} 1 & -1 & 2 \\ -1 & 3 & -2 \\ 2 & -2 & 2 \end{pmatrix}.$$

with $\det \text{Watson}(A) = -2^2$.

The direct calculation of the automorphism group of A takes about 71 seconds while using the Watson process gives the result in next to no time. For A , the algorithm finds 16 inequivalent D -perfect points, for $\text{Watson}(A)$ there is only one. This and the reduction of the determinant by a factor 15^2 explains this difference.

4.1 Statistics

Since we can not estimate the running time for our algorithm, we would like to give some statistics. For this purpose, we randomly chose 1000 integral hyperbolic 3×3 matrices with entries between -25 and 25 and determinant ≥ -200 and measured the time (in seconds) needed to compute every single automorphism group, once applying the Watson process (row Watson I), once not (row no Watson I), where for both tests we used the same list of matrices to allow direct comparison. To emphasize the strong effect of the Watson process we did the same thing with 1000 integral hyperbolic matrices, for which the Watson process really changes the matrix (rows no Watson II and Watson II). We also compared two runs where we required the tested matrices to be isotropic and anisotropic respectively (whereas we applied the Watson process in both cases). Table 1 gives the statistics. The value in brackets behind the average values is the standard deviation of the data.

	\emptyset Time (sec.)	min./max. Time (sec.)	\emptyset # Points	min./max. # Points
no Watson I	95.45 (212.57)	0.01 / 1263.99	9.7 (9.0)	1 / 44
Watson I	68.86 (195.11)	0.01 / 1240.99	7.6 (8.8)	1 / 44
no Watson II	70.08 (178.92)	0.02 / 1623.69	7.4 (6.7)	1 / 34
Watson II	2.96 (26.64)	0.01 / 481.62	2.7 (2.3)	1 / 15
Isotropic	98.18 (223.73)	0.01 / 1285.13	8.9 (10.3)	1 / 44
Anisotropic	2.43 (3.67)	0.01 / 37.36	5.1 (3.8)	1 / 18

Table 1: Computational statistics

Apparently, automorphism groups of anisotropic lattices are - in a way - far easier to compute than the ones of isotropic lattices. This phenomenon occurred while testing the implementation of our algorithm, but we cannot really explain it. However, this also shows the significance of the usage of the Watson process, because, heuristically, the Watson process affects about 50% of all isotropic forms of rank 3, while it only affects about 30% of all anisotropic forms and the computation for anisotropic forms is much faster anyway.

Acknowledgements

Some of the ideas presented in Section 3 of this paper are already due to Opgenorth and are contained in preliminary and unpublished versions of [13] which the author was kindly allowed to use.

He wants to thank Prof. Gabriele Nebe and Markus Kirschmer for reading a first draft of this paper and their helpful suggestions, David Lorch and again Markus Kirschmer for their help with the MAGMA implementation of the algorithm.

References

- [1] Daniel Allock. The Reflective Lorentzian Lattices of Rank 3. *Memoires of the American Mathematical Society*, 2012.
- [2] Amitabh Basu, Michele Conforti, Gérard Cornuéjols, and Giacomo Zambelli. Maximal Lattice-Free Convex Subsets in Linear Spaces. *Trepper School of Business*, (63), 2009.
- [3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I The user language. *Journal of Symbolic Computation*, 24:235–265, 1997.
- [4] John Horton Conway and Neil James Alexander Sloane. *Sphere Packings, Lattices and Groups*. Springer-Verlag, 1988.
- [5] Warren Dicks. *Groups, Trees and Projective Modules*. Springer-Verlag, 1980.
- [6] David-Olivier Jaquet-Chiffelle. Trois Théorèmes de finitude pour les G -formes. *Journal de Théorie des Nombres de Bordeaux*, 7(1):165–176, 1995.
- [7] Max Koecher. Positivitätsbereiche im \mathbb{R}^n . *American Journal of Mathematics*, 79:575–596, 1957.
- [8] Max Koecher. Beiträge zu einer Reduktionstheorie in Positivitätsbereichen I. *Mathematische Annalen*, 141:384–432, 1960.
- [9] David Lorch. Einklassige Geschlechter positiv definiter Gitter in Dimension 3. Master’s thesis, RWTH Aachen University, 2012.
- [10] Michael H. Mertens. Duale Kegel und Automorphismengruppen hyperbolischer Gitter. Master’s thesis, RWTH Aachen University, 2012.
- [11] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, 2007.
- [12] Jürgen Opgenorth. *Normalisatoren und Bravaismannigfaltigkeiten endlicher unimodularer Gruppen*. Aachener Beiträge zur Mathematik, 1996.
- [13] Jürgen Opgenorth. Dual Cones and the Voronoi-Algorithm. *Experimental Mathematics*, 10(4):599–608, 2001.
- [14] Jürgen Opgenorth, Wilhelm Plesken, and Tilman Schulz. Crystallographic Algorithms and Tables. *Acta Crystallographica*, A54:517–531, 1998.
- [15] Wilhelm Plesken and Bernd Souvignier. Computing Isometries of Lattices. *Journal of Symbolic Computation*, 24:327–334, 1997.
- [16] Michael Pohst and Hans Zassenhaus. *Algorithmic algebraic number theory*. Cambridge University Press, 1989.
- [17] Jean-Pierre Serre. *Trees*. Springer-Verlag, 1980.

- [18] Carl Ludwig Siegel. Einheiten quadratischer Formen. *Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität*, 13:209–239, 1940.
- [19] Ernest Borissowitsch Vinberg. On groups of unit elements of certain quadratic forms. *Mathematics of the USSR Sbornik*, 16(1):17–35, 1972.
- [20] Georgi Feodosjewitsch Voronoi. Nouvelles applications des paramètres continus à la théorie des formes quadratiques: 1 sur quelques propriétés des formes quadratiques positives parfaites. *Journal für die Reine und Angewandte Mathematik*, 133:97–178, 1908.
- [21] George Leo Watson. Transformations of a quadratic form which do not increase the class number. *Proceedings of the London Mathematical Society*, 3(12):577–587, 1962.